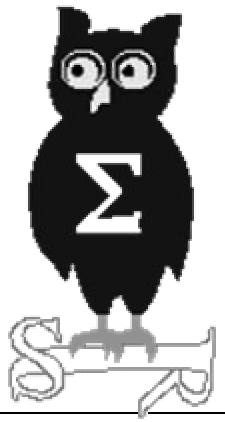
OSSIR
Groupe Sécurité Windows

Réunion du 17 décembre 2001



Durcissement Windows 2000

Contrôleur de Domaine (DC)

- Maxime de Jabrun
- mdejabrun@edelweb.fr

Sommaire

- **Périmètre de la présentation**
- **Concepts**
- **Sécurisation**

Périmètre

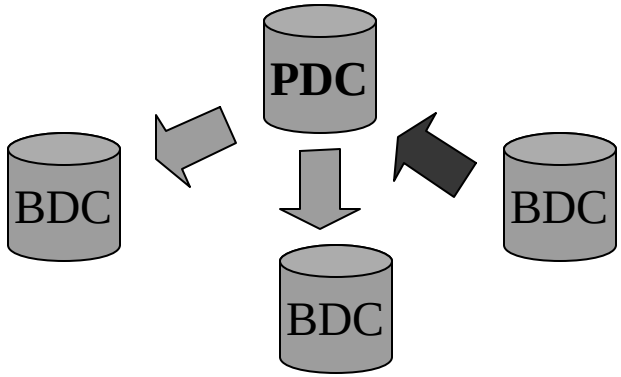
- Sécurisation d'un contrôleur de domaine standard (aucun rôle spécial)
- Mode natif (quelques précisions en mode mixte à titre indicatif)
- Il ne s'agit pas d'une checklist mais de présenter les services de sécurité proposés par Windows 2000 et quand cela est nécessaire, de préciser les points de configuration importants qui s'appliquent à un DC

Concepts

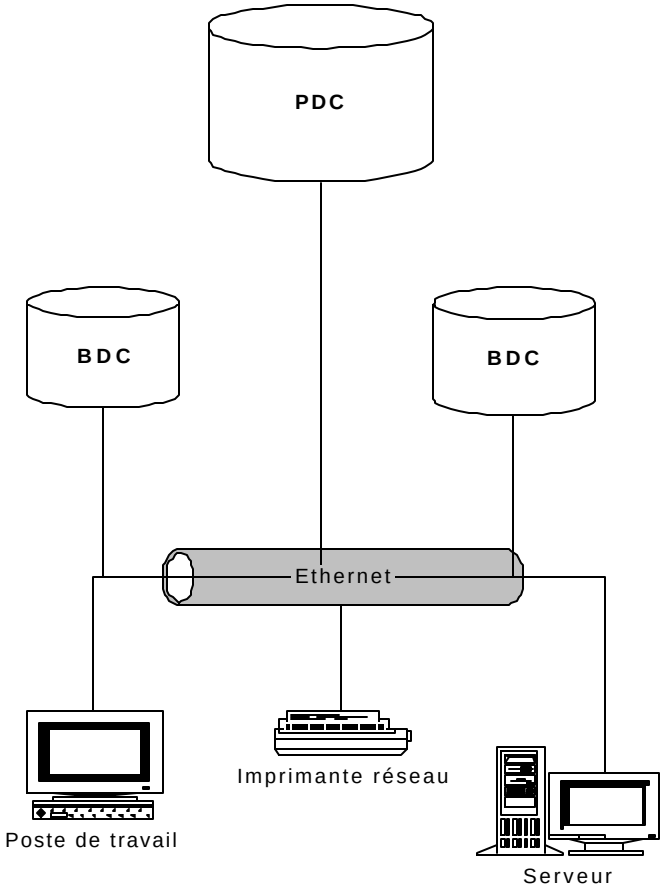
- Rappels NT4
- Rôles d’un DC – Windows 2000
- Stratégies de groupe – GPO (Group Policy Object)

Rappel NT4

- Le périmètre de sécurité: domaine
- Le centre nerveux: le contrôleur principal (PDC: Primary Domain Controler)
- Secondé par des contrôleurs secondaires (BDC: Backup Domain Controler)



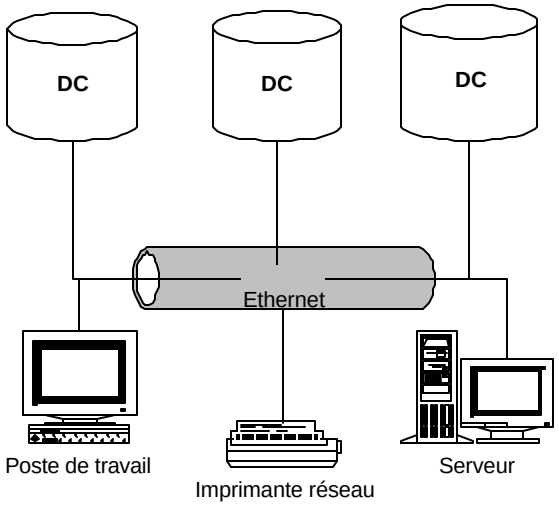
Rappel NT4


PDC
BDC
BDC
Ethernet
Imprimante réseau
Poste de travail
Serveur

Le DC sous Windows 2000

- Le périmètre de sécurité: la forêt
  - Domaines reliés par des relations d'aprobation bidirectionnelles
- Le centre nerveux: Active Directory
- Partagé par tous les contrôleurs du domaine

DCs équivalents



Les rôles d'un DC

- Flexible Single Master Operation : les rôles FSMO
  - Schema master (un par forêt)
  - Domain naming master(un par forêt)
  - RID master(un par domaine)
  - PDC master (un par domaine)
  - Infrastructure master (un par domaine)
- Déterminer les rôles des DCs, Kit de ressources:
  - netdom query fsmo
  - Dumpfsmos.cmd

Rôles: KDC

- Key Distribution Center (KDC) :service de domaine.
  - Utilise AD comme base de comptes
  - le Global Catalog fournit les pointeurs vers les KDCs des autres domaines
- Le KDC d'un domaine est installé sur un DC tout comme AD. Les deux services sont démarrés automatiquement par la LSA (Local Security Authority)
- Un DC peut accepter les demandes d'authentification et de TGS adressées au KDC du domaine

GPO 1- application

- Ordre d’application
  - L’unique LGPO
  - Les stratégies de Site dans l’ordre administratif
  - Les stratégies de domaine, dans l’ordre administratif
  - Les stratégies d'UO des plus englobantes au plus fines (des parents aux enfants),dans l’ordre administratif au niveau de chaque UO
- Les stratégies de compte ne sont applicables qu'au niveau du domaine!

GPO 2 - application

- Il est possible pour une UO de forcer une stratégie à ses enfants: “No Override”
- Une gpo machine est chargée au démarrage de la machine
- Pour un utilisateur elle est chargée au logon
- Elles sont mises à jour toutes les 90 minutes

GPO 3 - stockage

- LGPO : %systemroot%\system32\GroupPolicy
  - gpt.ini, administrative templates (.adm), security configuration files (.pol) et les scripts de logon/off startup/shutdown
- ADGPO :

  %systemroot%\system32\sysvol\<domain>\Policies et un pointeur vers chaque ADGPO est stocké dans l'annuaire dans le conteneur system >> Policy

Sécurisation

- Installation
- Protection des composants Windows 2000
- Configuration
  - Utilisateurs
  - Services
  - Permissions

Installation 1

- Installer un Server US en mode complet et pas « en copie » avec les derniers SP, hot fixes
- NTFS
  - Désactiver EFS: HKLM\SYSTEM\CCS\Control\FileSystem\ effacer la valeur NtfsEncryptionService
- Créer plusieurs partitions
  - Système
  - Applications
  - journaux

Installation 2

- Utiliser DCPROMO.EXE pour promouvoir le serveur en contrôleur de domaine
- Choix de compatibilité de permissions
  - Selon le mode (pre windows 2000 pour mode mixte)
- Installer le minimum de services
- Désinstaller les sous systèmes OS2/posix
- Désinstaller le support netware
- Désactiver les partages administratifs et l'accès distant à la base de registre

Active Directory: AD

- Les fichiers à protéger
  - Les répertoires et leurs sous répertoires
    - %SystemRoot%\SYSVOL
    - %SystemRoot%\System32\GroupPolicy
  - Le fichier
    - %SystemRoot%\NTDS\ntds.dit
- Utiliser SSL:
  - serveur: Q247078, Port 636 - ldap ssl et 3269 - GC SSL
  - client: Q238007
- Eviter la délégation d'administration sur les DC (Administration delegation)
- L'outil de backup doit prendre en compte la registry et AD: ntbackup

Résolution de nom: DNS

- Client: cache les requêtes
  - %WinDir%\system32\config\Netlogon.dns acl Admin,syst: possède les enregistrements SRV
  - Forcer la résolution de nom par DNS en premier (Services\tcpip\ServiceProvider\DNSPriority)
- Serveur, 2 solutions: MS, BIND
  - BIND
  - MS: Blinder, 1 serveur DNS par forêt, un sous domaine dédiée AD

Réplication

- 2 modes de réplication
  - Smtp
    - Inter site ET inter domaine
    - Asynchrone
    - Pour les DCs de rôle schema, configuration, et global catalog
  - Knowledge Consistency Checker (KCC)
    - Intra site (ou inter site)
    - Synchrone
    - Les DCs doivent être correctement déclarés
- Ipsec
  - en mode transport
  - trafic DC<-> DC et global catalog <-> global catalog (Q254949)
- Incompatibilité avec NAT (tickets kerberos non valides)

Secure channel

- Q128489: secure channel entre DC de domaines différents, compte machine utilisé
- Renforcer le canal de communication
  - HKLM\SYSTEM\CurrentControlSet\Services\NetLogon\Parameters\SealSecureChannel\REG_DWORD:1
  - HKLM\SYSTEM\CurrentControlSet\Services\NetLogon\Parameters\SignSecureChannel=REG_DWORD:1
  - HKLM\SYSTEM\CurrentControlSet\Services\NetLogon\Parameters\RequireSignOrSeal=REG_DWORD:1
  - HKLM\SYSTEM\CurrentControlSet\Services\NetLogon\RequireStrongKey=REG_DWORD:1

Authentification: Kerberos

- Ne peut être imposé, sauf si la stratégie Ipsec- Secure Server (Require Security) est assigné à tous les serveurs du domaine
- Q254728;HKLM\SYSTEM\CCS\Services\IPSEC
  - NoDefaultExempt = 1: RSVP et Kerberos Le client et le serveur doivent se trouver dans la même forêt
- Le client doit désigner le serveur par son nom DNS
  - Net use \\IP@\c$ n'utilisera pas Kerberos
- La clé utilisée pour distribuer la clé de session est le hash du mot de passe de l'utilisateur client
- Renforcer les restrictions: Enforce User Logon Restrictions
- Utiliser la pré-authentification Kerberos

Authentification: ntlm

- réglage du niveau de sécurité de l'authentification: ntlmv2 (Q239869)
  - Lmcompatibility level :
    - 3 sur les clients
    - 4 sur les Dcs
  - NtlmMinClientSec
    - 0x00000010- Message integrity
    - 0x00000020- Message confidentiality
    - 0x00080000- NTLM 2 session security
    - 0x20000000- 128-bit encryption
    - 0x80000000- 56-bit encryption

WFP (SFP)

- Windows (ou System) File Protection
- Limites:
  - WFP peut être désactivé de façon permanente HKLM\swt\MS\Windows NT\CV\Winlogon SFCDisable 0ffffff9dh
  - Si la signature du fichier en cours de vérification correspond à une signature de la liste alors le fichier n'est pas mis à jour (ex: copy notepad.exe wscript.exe)
  - Un boot en mode recovery console permet de modifier les fichiers sans que le système ne réagisse
- Recommandation
  - Mettre des ACLs restrictives plutôt que d'effacer un fichier

Journalisation

- Créer une partition séparée pour les journaux HKLM\SYSTEM\CurrentControlSet\Services\EventLog\<journal>\File
- Attention au problème de remplissage des journaux (crashonauditfail = 2)
- Auditer en échec seul Directory Access, en succès et échec tous les autres événements sauf Process Tracking
  - Audit Logon, audit account logon
- Surveiller les événements: Auditing Disabled
- Restrict guest access (gpo)

Fin de la première partie

- Deuxième partie
  - Configuration des comptes
  - Services
  - permissions

Comptes - Liste des groupes

- Groupes Universels (mode natif uniquement):
  - Schema Admins
  - Enterprise Admins
- Groupes Globaux:
  - Domain Admins
  - Domain Users
  - Domain Guests
- Groupes Locaux:
  - Administrators
  - Replicators devrait être vide
  - Backup Operators
  - Server Operators
  - Print Operators
  - Account Operators
  - Guests
  - Users

- Remarque: certains services, comme Terminal Service, ajoutent des comptes spécifiques
- Inclusions: groupes Universels, Globaux, Locaux

Comptes - Création et gestion

- Créer un groupe userAdmin membre de Users
  (pour lancer des commandes telles que runas)
- Créer les comptes à partir de modèles (copier)
- Préférer Users (et non pas power users)
- Retirer Everyone du groupe: pre-windows 2000 Compatible Access (utilisé pour RAS et SQL pré 2K q240855) en mode mixte
- Placer le groupe Administrators dans les groupes restreints

Comptes - stratégie

- Compte administrator
  - Renommer
  - Créer un leurre
  - Mot de passe très robuste.
  - Passprop -> admnlock.exe; Q279672
- forcer le déverrouillage d'un compte par un administrateur
- Limiter les droits d intervention sur les DC aux administrateurs seuls

Mots de passe - stockage

- Ne pas stocker le hash LM dans AD ni dans la sam (uniquement le compte local de restore mode sur un DC)
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\NoLMHash = 1 (REG_DWORD)
  - Changement de mot de passe des stations 9x et authentification sans DSCLIENT : dysfonctionnement
- Pas de mot de passe en clair EnablePlainTextPassword = 0
- Pas de cache de mot de passe
  HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
  CachedLogonsCount = 0
- Un mot de passe de 15+ caractères n'est pas stocké LM

Mots de passe - gestion

- Mot de passe Administrator du Restore Directory Service Mode (SAM, NULL via l'ihm)
- Mot de passe du compte machine
  - Il est aléatoire (dès l'installation), et renouvelé
  - HLM\SYSTEM\CurrentControlSet\Services\NetLogon\Parameters\ MaximumPasswordAge (REG_DWORD)
    - Default = 30
    - Range = 1 to 1,000,000 (jours)

    ->Impact sur la charge réseau

- Exigences de complexité dans la stratégie de comptes

Privilèges et droits:

- Interactive logon : restreindre l'accès interactif aux seuls comptes les plus sûr (Administrators et leurs comptes utilisateurs)

- Accès from network, Bypass Traverse Checking: tous les utilisateurs du domaine

Services 1

- Base de services indispensables sous Windows 2000:
  - Event Log
  - Logical Disk Manager
  - Plug&Play
  - Protected Storage
  - Security Account Manager

Services 2

- Services utiles
  - IPSec Policy Agent
  - Network Connections Manager
  - Remote Procedure Call
  - RunAs Service
  - Netlogon
  - Workstation (nécessaire pour Netlogon)
  - TCP/IP Netbios Helper (mode mixte)

Services 3

- Services supplémentaires requis sur un DC
  - DNS Server (au moins un serveur DNS supportant les mises à jour dynamiques est nécessaire sur le domaine)
  - File Replication Service (si pls DC)
  - Kerberos Key Distribution Center
  - NT LM Service Provider
  - RPC Locator
  - Windows Time
  - Computer Browser (mode mixte)
  - Server (si ressources partagées ou si AD est démarré)
  - Workstation (si le DC se connecte à des ressources)

Services 4

- Services à proscrire si possible
  - Remote Installation Service
  - Remote Registry Service
  - Alerter
  - Application Management
  - DHCP client
  - DHCP Server
  - DNS client
  - SNMP Trap Service
  - ClipBook Server
  - Telnet Server
  - RRAS
  - IIS et services associés
  - Telephony
  - Printing spooler

Services 5: Mesures

- Sécurisation / désactivation de SMB
  - Désactiver le composant file and printer sharing (impact fonctionnel important si les GPO sont utilisées, les stratégies ne seront plus accessibles)
  - forcer SMB over TCP (Direct Hosting) sans l aide de NetBT (“netbios over tcp/ip” décochée)
  - RestrictAnonymous = 2 | “Additional restrictions for anonymous connections” et paramètres de restriction d'accès en null session
- Utiliser le compte Local System ou un compte dédié au service
  - Faire tourner un service sous le contexte d'un compte permet à un administrateur de récupérer le mot de passe associé (stocké dans les secrets LSA)

Ports utilisés

- Réseau entièrement Windows 2000

Client Port(s)	Server Port	Service
> 1024 /TCP	135/TCP	RPC *
> 1024 /TCP /UDP	389/TCP/UDP	LDAP
> 1024 /TCP	636/TCP	LDAP SSL
> 1024 /TCP	3268/TCP	LDAP GC
> 1024 /TCP	3269/TCP	LDAP GC SSL
53,> 1024 /TCP /UDP	53/TCP/UDP	DNS
> 1024 /TCP /UDP	88/TCP/UDP	Kerberos
> 1024 /TCP	445/TCP	SMB

- Réseau mixte (NT et 2000) rajouter les suivants

Client Port(s)	Server Port	Service
> 1024 /TCP	135/TCP	RPC *
137/UDP	137/UDP	NetBIOS Name
138/UDP	138/UDP	NetBIOS Netlogon and Browsing
> 1024 /TCP	139/TCP	NetBIOS Session
> 1024 /TCP	42/TCP	WINS Replication

Mécanismes de démarrage d'applications

- Méthodes
  - Utilisation de clés de démarrage
  - Utilisation des fichiers et répertoires de démarrage.
  - Détournement du shell
- Mesures de protections:
  - restriction de permission d’accès (ACL)
  - surveillance particulière (audit, host IDS)

Permissions fichier

- Renforcées par rapport à NT
- Quelques commandes de system32 peuvent faire l'objet d'un durcissement d'ACL
- Les fichiers dll, drv, sys, ocx, exe, com, scr, bat, cmd, cpl dans %SystemRoot, System et System32 doivent être en lecture seule pour les utilisateur authentifié

Conclusion

- Sécurité: une préoccupation forte de Windows 2000
- Gestion centralisée de la sécurité sur les DCs
- Le contrôleur de domaine est plus que jamais le point clé de la gestion et de la sécurité du domaine

Références

- Guides et modèles de sécurisation de la NSA
- Guide du SANS
- Knowledge Base, MSDN, Resource Kit
- Edelscope, Edelweb